AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

United States of America
v.

JOSHUA FORD

Defendant(s)

Case No. 3:19mj256

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 6/23/2018 in the county of Montgomery in the Southern District of Ohio, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)(B) & 18 U.S.C. § 2252A(a)(2)	Distribution of Child Pornography
18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B)	Possession of Child Pornography

This criminal complaint is based on these facts:

See Attached Affidavit

☑ Continued on the attached sheet.

Complainant's signature

SA Kimberly Wallace, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 5-6-19

Judge's signature

City and state: Dayton, Ohio

Hon. Sharon L. Ovington, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Kimberly Wallace, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with Immigration and Customs Enforcement, Homeland Security Investigations (HSI) and have been so employed since 2010. I am currently assigned to the HSI Resident Agent in Charge Cincinnati, Ohio office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a), and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.

2. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents and officers involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge. Based on the investigation conducted to date, there is probable cause to believe that Joshua FORD received or distributed child pornography, in violation of 18 U.S.C. §§ 2252(a)(2)(B) and 2252A(a)(2), and possessed child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B). I submit this Affidavit in support of a criminal complaint.

PERTINENT FEDERAL CRIMINAL STATUTES

3. 18 U.S.C. § 2252(a)(2)(B) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mail if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

4. 18 U.S.C. § 2252A(a)(2) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign

commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

5. 18 U.S.C. § 2252(a)(4)(B) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

6. 18 U.S.C. § 2252A(a)(5)(B) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

BACKGROUND INFORMATION

Definitions

7. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "Chat" refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child Pornography" is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

c. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves, obscene or

illegal. In contrast to "child pornography," this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries. See Kenneth V. Lanning, Child Molesters: A Behavioral Analysis (2001) at 65. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child pornography cases. See United States v. Cross, 928 F.2d 1030 (11th Cir. 1991) (testimony about persons deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant); United States v. Riccardi, 258 F.Supp.2d 1212 (D. Kan., 2003) (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).

d. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

e. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

f. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

g. "Cloud-based storage service" refers to a publicly accessible, online, storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

h. "Computer" means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. § 1030(e)(1).

i. "Computer hardware" consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic,

magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices), peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

j. "Computer software" is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic or other digital form. It commonly includes programs to run operating systems, applications and utilities.

k. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software or other related items.

l. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

m. "File Transfer Protocol" ("FTP") is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

n. "Internet Service Providers" (ISPs) are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage and co-location of computers and other communications equipment. ISPs can offer various means to access the Internet, including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or

screen name, an e-mail address, and an e-mail mailbox and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

o. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

p. "Internet Protocol address" (IP address) refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

q. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

r. The terms "records," "documents" and "materials" include all information recorded in any form, visual or aural, and by any means, whether in hand-made form (including writings, drawings, painting), photographic form (including microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including phonograph records, printing, typing) or electrical, electronic or magnetic form (including tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

s. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

t. "Digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including the following: central processing units; laptop or notebook computers; PDAs; wireless communication devices such as telephone paging devices, beepers and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors and drives intended for removable media; related communications devices such as modems, cables and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips; and security devices.

u. "Image" or "copy" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.

v. "Hash value" refers to a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data.

w. "Steganography" refers to the art and science of communicating in a way that hides the existence of the communication. It is used to hide a file inside another. For example, a child pornography image can be hidden inside another graphic image file, audio file or other file format.

x. "Compressed file" refers to a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

y. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of www.usdoj.gov refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters with each level delimited by a period. Each level, read backwards from right to left further identifies parts of an organization. Examples of first level or top level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second level names will further identify the organization. For example, usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the world wide web server located at the United States Department of Justice, which is part of the United States government.

z. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

aa. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

bb. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper Text Mark up Language (HTML) and is transmitted from web servers to various web clients via Hyper Text Transport Protocol (HTTP).

cc. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

KIK MESSENGER APPLICATION

8. The Kik Messenger application is primarily a social media mobile device platform designed and managed by Kik Interactive Incorporated, a Waterloo, Canada based company, for the purpose of mobile messaging and communication. To use this application, a user downloads the mobile messaging application via an applications service such as the Google Play Store, Apple iTunes, or other similar mobile application provider. Once downloaded and installed, the user is prompted to create an account and a username. This username will be the primary account identifier. The user also has a display name, which will be what other users initially see when transmitting messages back and forth. As part of the account creation process, Kik users are asked to supply a valid email address, create a password, provide an optional date of birth, and user location. The user also has the option of uploading a "profile avatar" that is seen by other users. Once the Kik user has created an account; the user is able to locate other users via a search feature. The search feature usually requires the user to know the intended recipient's username. Once another user is located or identified, Kik users can send messages, images, and videos between the two parties.

9. Kik Messenger also allows users to create chat rooms, of up to 50 people, for the purpose of communicating and exchanging images and videos. These rooms are administered by the creator who has the authority to ban and remove other users from the created room. According to Kik Messenger, more than 40% of the Kik users chat in "groups" and approximately 300,000 new groups are created every day. These groups are frequently created with a "hashtag" allowing the group or chat to be identified more easily. Once the group or chat is created Kik users have the option of sharing the "link" with all of their contacts or anyone they wish.

FACTS SUPPORTING PROBABLE CAUSE

10. In the instant matter, KIK Interactive, Inc., an electronic service provider, provided reports of Child Sexual Abuse Material (CSAM) to the Royal Canadian Mounted Police (RCMP). The RCMP filtered the content and provided referrals relating to U.S. users to HSI Ottawa, Canada. HSI Ottawa received from the RCMP, KIK user information as well as content sent by the user. HSI Ottawa filtered the KIK user information to determine the suspect's geolocation based upon the user's IP address login. HSI Ottawa then disseminated leads to HSI domestic offices. Kik reports user content under four (4) categories: Abuse, Other, SafePhoto and PhotoDNA.

11. In September 2018, HSI Cincinnati received a referral from HSI Ottawa for KIK user "joeangie37" which was reported by KIK for CSAM. The referral included KIK subscriber records, user information, a SafePhoto report and an image uploaded for the account. I reviewed the information for "joeangie37" and identified the IP address with a date and time associated with the upload of CSAM. KIK user "joeangie37" uploaded content at IP address 65.186.28.150 on June 23, 2018, at 06:31:16 UTC. The image depicted child pornography and is described as follows:

    a. The image depicted a naked pre-pubescent female, showing from her ear down, sitting on what appears to be a bed, with her legs spread exposing her genitals. There is an adult male, showing from his pelvis down, standing in front of her wearing white underwear pulled down to his thighs, with an erect penis. The pre-pubescent female has the male's erect penis partially in her mouth.

12. I performed a query of IP address 65.186.28.150 and found that the ISP was listed as Spectrum (Charter Communications, Inc).

13. On approximately September 11, 2018, I served a Department of Homeland Security summons on Charter Communications, Inc., requesting subscriber records for IP address 65.186.28.150 for June 23, 2018, at 06:31:16 UTC, the date/time indicated by KIK for the uploaded image (described in paragraph 11a). On approximately September 14, 2018, I received a response from Charter Communications indicating the subscriber was located at 2530 Columbus Ave, Rear, Apt. Rear, Springfield, OH 45503-3551.

14. After a review of subscriber information for "joeangie37", I observed that the most recent login IP address for the user was different from the image upload IP address. The most recent account access for user "joeangie37" was on June 24, 2018 at 15:04:58 UTC from IP address 99.34.1.87.

15. I performed a query of IP address 99.34.1.87 and found that the ISP was listed as AT&T U-Verse (AT&T Services, Inc.).

16. On approximately September 11, 2018, I served a Department of Homeland Security summons on AT&T, Inc., requesting subscriber records for IP address 99.34.1.87 for June 24, 2018, at 15:04:58 UTC, the date/time indicated by KIK for the most recent account access for "joeangie37". On approximately September 14, 2018, I received a response from AT&T indicating the subscriber was located in Springfield, OH.

17. I conducted an internet query of the subscriber address provided by AT&T and results indicated a convenience store at the address (hereinafter referred to as "Business A").

18. On approximately March 6, 2019, HSI Special Agents located a business ("hereinafter referred to as "Business B") and two apartment units located on-site at 2530 Columbus Avenue, Rear, Springfield, OH. HSI agents spoke to personnel in the office of Business B and were told that the occupants of the apartments on-site (2530 Columbus Ave, Rear), also worked at Business B. HSI agents asked to speak to one of the apartment residents.

19. HSI Special Agents spoke to Joshua FORD, one of the apartment residents. Agents told FORD he was not under arrest.

20. FORD claimed to have lived at 2530 Columbus Ave, Rear, Apt 2, Springfield, OH for approximately five (5) years. FORD stated he utilized the internet at the location which was password protected.

21. FORD stated he worked at Business B for approximately seven (7) years.

22. FORD stated he also worked at Business A (as referred to in paragraph 17) periodically for approximately the past three (3) years.

23. FORD stated that he had previously been interested in child pornography but not currently. FORD stated that he would receive child pornography and would also send child pornography to unknown people via the internet.

24. FORD stated he only traded child pornography images and never produced any images or videos depicting child pornography.

25. FORD stated he had a KIK account and recognized the name "joeangie37" when HSI agents asked. FORD stated he remembered the account and named it as such because the

name sounded humorous, "jo mamma and jo daddy". FORD stated that he traded child pornography on KIK.

26. FORD stated that at some point, he was unable to log into the KIK account. FORD stated he tried to reset the password to which he received a message that stated his account was banned.

27. FORD stated he currently had one (1) tablet that he had utilized to trade child pornography. FORD stated he purchased the tablet in approximately December 2017. FORD stated that there currently might be one (1) image depicting child pornography on tablet. FORD stated that there had been more images of child pornography on tablet, but those images were possibly gone. FORD stated the tablet was located in the office of Business B. FORD said the tablet was not password protected.

28. HSI Special Agents followed FORD to the business office and seized the tablet.

29. On or about April 9, 2019, Your Affiant applied for and was granted a search warrant for FORD's tablet.

30. On or about April 11, 2019, a HSI Computer Forensics Special Agent executed the above-referenced search warrant on FORD's tablet. An extraction report was provided to Your Affiant.

31. On or about April 17, 2019, Your Affiant reviewed material located on FORD's cellular telephone from a forensics extraction report and observed the following:

a. An image titled "avatar_user499473_7124853573940826.jpg" and depicted a prepubescent female wearing only a shirt and partially lying on a bed with her back on a pillow. The female's legs are spread exposing her genitals.

b. An image titled "imgcache.0_embedded_164.jpg" and depicted a prepubescent female lying on a blanket wearing only black thigh-high stockings. There appeared to be yellow rope tied around her left ankle and left thigh and yellow rope tied around her right ankle and right thigh exposing her genitals. There also appeared to be yellow rope tied around her wrists which were pulled above her head.

c. An image titled "imgcache.0_embedded_310.jpg" (appeared similar to the photograph described in paragraph 11a) and depicted a naked pre-pubescent female, showing from her ear down, sitting on what appears to be a bed, with her legs spread exposing her genitals. There was an adult male, showing from his pelvis down, standing in front of her wearing white underwear pulled down to his thighs, with an erect penis. The pre-pubescent female had the male's erect penis partially in her mouth.

CONCLUSION

32. Based on the evidence described in this affidavit and my experience and training, and the experience and training of law enforcement personnel with whom I have discussed this case, there is probable cause to believe that on or about June 23, 2018, in the Southern District of Ohio, Joshua FORD knowingly distributed child pornography in violation of Title 18 U.S.C. §§ 2252(a)(2)(B) and 2252A(a)(2).

33. Based on the evidence described in this affidavit and my experience and training, and the experience and training of law enforcement personnel with whom I have discussed this case, there is probable cause to believe that on or about March 6, 2019, in the Southern District of Ohio, Joshua FORD possessed child pornography in violation of Title 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B).

Kimberly Wallace
Special Agent
Homeland Security Investigations

SUBSCRIBED and SWORN
before me this 6th of May 2019

SHARON L. OVINGTON
UNITED STATES MAGISTRATE COURT JUDGE